DOCUMENT RESUME

ED 472 092 SE 066 375

AUTHOR	Rousseau, Christiane
TITLE	Mathematics: A Living Discipline within Science and Technology.
PUB DATE	2001-00-00
NOTE	11p.; In: Canadian Mathematics Education Study Group = Groupe Canadien d'Etude en Didactique des Mathematiques. Proceedings of the Annual Meeting (25th, Edmonton, Alberta, Canada, May 25-29, 2001); see SE 066 374.
PUB TYPE	Reports - Descriptive (141) -- Speeches/Meeting Papers (150)
EDRS PRICE	EDRS Price MF01/PC01 Plus Postage.
DESCRIPTORS	*Course Descriptions; Foreign Countries; Higher Education; Interdisciplinary Approach; *Mathematical Applications; *Mathematical Models; *Mathematics Instruction; Mathematics Teachers; Preservice Teacher Education; Teacher Education Programs
IDENTIFIERS	*Canada

ABSTRACT

This paper presents information on a course entitled "Mathematics and Technology" which was created at the University of Montreal and was taught once during the winter term of 2001. The students in the course were for the most part future high school teachers. Several applications of mathematics in technology are introduced and students are reminded throughout the course that mathematics is present everywhere in new technologies, mathematics is alive and new developments occur all of the time, and with mathematical tools and problem solving skills, anyone can contribute to technology. (KHR)

Mathematics, A Living Discipline within Science and Technology

Christiane Rousseau
Université de Montréal

The purpose of this paper is to present a new course « Mathematics and technology » which was created at the Université de Montréal and has been taught once during the winter term of 2001. The students in the course were for the most part future high school teachers. A few students in applied mathematics also attended the course.

The objective of the course is to introduce to several applications of mathematics in technology. The applications chosen are:

- very modern for the most part;
- using relatively elementary mathematics;
- but some sophistication is needed to get extra power.

In the course the students have to do:

- mathematical modeling;
- problem solving;
- use of computers (but not for all applications);
- a project (similar to the projects done in science fairs).

Around 12 applications are studied, for usually five hours each:

- Elementary theory (one hour);
- Exercises (2 hours);
- Advanced theory (2 hours).

For the evaluation the students have to do:

- 3 half-exams half take-home (mostly on the elementary parts);
- a project (report of 25 pages) plus an oral presentation (30 minutes). The students work by teams of 2.

Throughout the course the students find the following messages:

- mathematics are everywhere present in new technologies;
- mathematics are alive and new developments occur all the time;
- with mathematical tools and problem solving skills anyone can contribute to technology, BUT programming is also an essential tool.

A guided tour of some applications (not all elementary)

The purpose of the guided tour is to show how numerous are the applications of mathematics.

Applications in health

- Cardiac arrythmias and chaotic dynamics: Mathematicians and cardiologists work together to better understand the mechanisms of the heart and the onset of chaos. The hope is to be able to control arrythmias with pacemakers;
- Pharmacy: how to better control the diffusion of drugs so as to be able to give smaller quantities and minimize side effects;

- Medical imaging: wavelets allow to "clean" an image to get a better diagnosis;
- Medical imaging: reconstruction of 3D-images from 2D-images.

Applications in molecular biology

- Knot theory is used to explain the action of enzymes on DNA. [R]

Shape optimization

- Shape of a plane wing (aeronautics);
- Shape of a boat shell;
- Shape of a column. Let us recall the old problem posed by Lagrange: "find the shape of the stronger revolution column with fixed height and volume, under pressure from above". Lagrange "proved" that the strongest column is the cylinder. However Lagrange made a mistake and the strongest column was finally found by Cox and Overton in 1992. [C] If one reads Lagrange's work one cannot find the error as all his mathematical deductions are OK. The error lies in the fact that Lagrange erroneously supposed that the profile of the column was given by a differentiable function.

FIGURE 1: The optimal solution of Cox and Overton

Operational research

- Optimization in transport networks;
- Optimization in the distribution of cellular phone frequencies.

Shape recognition

- Reading of postal codes;
- Reading the amount of a check in an automatic teller;
- Recognition of voice;
- Recognition of finger prints;
- Vision of computers.

Financial mathematics

- Conception of derivatives.

Image compression

- Use of fractals.

Structural rigidity in architecture

Mathematics and music

- Clean a sound (for instance an old record);
- Compose new sounds on a synthetizer.

Cryptography

- Public key cryptography (RSA code for bank cards, internet);
- Quantic cryptography;
- The use of Penrose tilings for cryptography.

Engineering

- The movements of a robot.

Error correcting codes

DNA computers

Etc. ...

We will discuss in more details the following subjects:

- GPS;
- Public key cryptography;
- Error correcting codes;
- Image compression;
- Vision of computers;
- Movements of a robot.

There exist many more.

We start with a flash-science.

A remarkable property of the parabola

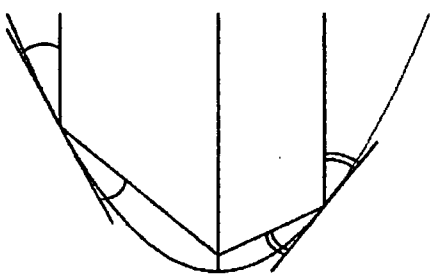

FIGURE 2: A remarkable property of the parabola

- When vertical rays are reflected they all meet in the same point (elementary).
- The parabola is the only curve with that property (more advanced: differential equation).
- Applications:

  Parabolic antenna;
  The mirror of a telescope;
  The shape of a radar;
  The shape of head-lights.

The GPS (Global positioning system)

The system was completely developed only in 1995 by the Ministry of Defense in United States, which allows the public to use it. 24 satellites move on orbits around the world, so that anyone on earth can catch the signals of at least 4 satellites.

The GPS gives one's position on earth. The principle is that the small receiver in one's hand measures the time necessary for a signal emitted by the satellite to travel from the satellite to the receiver. Given that the signal travels at the speed of light this allows us to

measure the distance from the satellite to the receiver: from this we know that the receiver is located on a sphere centered at the satellite. As three spheres intersect in 2 points the knowledge of the distance from the receiver to 3 satellites yields the position of the receiver since one intersection point is unrealistic.

This is theory. In practice the satellites have expensive atomic clocks which are perfectly synchronized while the receiver has a cheap clock. Then there is a fourth unknown: the clock offset, additional to the three unknowns for the position. Then the receiver needs a fourth measurement of the travel time from a fourth satellite to the receiver (the clock offset is the same for the 4 satellites). Here again we have a system of 4 equations with 4 unknowns which has 2 solutions, one of which is unrealistic.

This is the elementary theory. More advanced topics can be studied inside a project.

Examples:

- The use of differential GPS to get more precision (we compare with the travel time of the signal from the satellite to a second GPS located not too far and whose position is known to calculate exactly the speed of the signal since it does not travel in vacuum);
- The type of signal generated by the satellite: they are generated by shift registers using finite fields and have the property that they are very badly correlated to any other signal or to the signal translated;
- For other topics and details, see [GPS].

Applications:

- Finding one's way in wilderness;
- Drawing a map;
- Driving a plane in clouds and fog, etc.

Public key cryptography (RSA code 1978)

The basic ingredient is number theory, more precisely arithmetic (+,.) modulo n. We use the small Fermat theorem generalized by Euler.

The method works because theory and practice in number theory are very different:

- It is difficult (for a computer) to factor a large number;
- It is easy to create large prime numbers;
- It is easy to decide if a large number is prime.

Advantages of a public key system:

- There is no danger that the code becomes known! Hence it is the only possible code with millions of users.
- It is possible to "sign" a message in order to be sure it has been sent by the person who pretends having sending it.

The principle [RSA]:

- We choose p and q large prime numbers (more than 100 digits).
- We calculate $n = pq$. The number n, the "key", is public while p and q are kept secret.
- We calculate $\varphi(n)$, where φ is the Euler function defined as follows: $\varphi(n)$ is the number of integers in $\{1,2,...,n\}$ which are relatively prime with n. Then $\varphi(n) = (p-1)(q-1)$.
- Computing $\varphi(n)$ without knowing p and q is as hard as factoring n.
- We choose $e \in \{1,...,n\}$ relatively prime with n. e is the *encryption* key. It is public and allows the sender to encode the message.
- There exists $d \in \{1,...,n\}$ such that $ed \equiv 1 \pmod{\varphi(n)}$ (i.e., the rest of the division of ed by $\varphi(n)$ is 1. The existence of d follows from Euclid's algorithm to find the GCD of e and $\varphi(n)$. d is the *decryption* key. It is secret and allows the recipient to decode the message.
- The sender wants to send a message m which is a number in $\{1,2,...,n\}$, relatively prime

with n.
- He codes $m^e \equiv a \pmod{n}$, i.e., $a \in \{1,...,n\}$. He sends a.
- The recipient decodes. He calculates $a^d \pmod{n}$. The small theorem of Fermat, generalized by Euler, ensures that $a^d \equiv m \pmod{n}$.

Theorem of Euler:

If m is prime with n, then $m^{\varphi(n)} \pmod{n}$.
(Fermat had proved the theorem when n is prime.)

Consequence:

$$m^e \equiv a \pmod{n},$$
$$a^d \equiv (m^e)^d = m^{ed} = m^{b\varphi(n)+1} = m^{b\varphi(n)}.m = (m^{\varphi(n)})^b.m \equiv 1.m = m \pmod{n}.$$

Signature of a message: 2 public keys are necessary.

- Sender: n_A, d_A, public, e_A secret.
- Recipient: n_B, e_B, public, d_B secret.

To send a message m relatively prime with n_A and n_B:

$$m \mapsto m^{e_A} \equiv m_1 \pmod{n_A} \mapsto m_1^{e_B} \equiv m_2 \pmod{n_B}.$$

Then m_2 is sent.

To decode the message

$$m_2 \mapsto m_2^{d_B} \equiv m_1 \pmod{n_B} \mapsto m_1^{d_A} \equiv m \pmod{n_A}.$$

We have claimed that it is easy to construct large prime numbers. This follows from the prime number theorem which gives the asymptotic distribution of primes. To construct a prime number of 100 digits we generate random natural numbers with 100 digits and we test if they are prime. The prime number theorem ensures that after a mean of 125 trials we should get a prime (if we generate only odd numbers).

This means that there is a test for primality of a natural number n which is easier than to factor n. The test is technical and will not be discussed here. The underlying principle is that n leaves its "finger prints" everywhere so that if n is not prime then at least half the numbers in $\{1,...,n\}$ "know" that n is not prime. The test uses the Jacobi symbol. If k numbers $m_1,...,m_k \in \{1,...,n\}$ fail the test then n has a high probability of being prime (this is an exercise with Bayes formula). The number k need not be very high to yield a very large probability that n is prime (details in [RSA]).

Error correcting codes

Principle: We lengthen a message so that the information is contained in several places.

Example: We repeat each bit 3 times. If the 3 bits received are different we correct using the law of the majority, i.e., as if only one error has occurred. Then we recover the message if zero or one error has occurred. We say that the code corrects one error.

If we want to send a word of 8 bits we send 24 bits. As two different words have at least three different bits we get the right word if one error or less occurred.

We can do much better!

Hamming code:

We want to send a word of 4 bits: $u_1u_2u_3u_4$. We send a word of seven bits. We add

$$u_5 = u_1 + u_2 + u_3$$
$$u_6 = u_2 + u_3 + u_4$$
$$u_7 = u_1 + u_2 + u_4$$

This codes corrects one error. Indeed

No error	u_5, u_6, u_7 compatible
1 error in u_1	u_5, u_7 incompatible
1 error in u_2	u_5, u_6, u_7 incompatible
1 error in u_3	u_5, u_6 incompatible
1 error in u_4	u_6, u_7 incompatible
1 error in u_5	u_5 incompatible
1 error in u_6	u_6 incompatible
1 error in u_7	u_7 incompatible

We can do much better but with more sophisticated tools!

Reed-Solomon codes [RS]:

They use finite fields. The elements are words of n bits with an addition and a multiplication.

Example: The field K with 8 elements

The 8 elements can be identified with the 3-tuples whose entries are 0 and 1.

The addition of two 3-tuples is the 3-tuple whose entries are given by the addition of the respective entries modulo 2, i.e.,

$$(a_1, a_2, a_3) + (b_1, b_2, b_3) = (a_1 + b_1 \bmod 2, a_2 + b_2 \bmod 2, a_3 + b_3 \bmod 2,)$$

For multiplication we identify a 3 tuple (a_1,a_2,a_3) with the polynomial $a_1 + a_2x + a_3x^2$.
To reduce the product of two polynomials of degree ≤ 2 which is a polynomial of degree ≤ 4 we use the rule $x^3 = x + 1$. We deduce:

$$x^4 = x(x + 1) = x^2 + x$$
$$x^5 = x(x^2 + x) = x^3 + x^2 = (x + 1) + x^2 = x^2 + x + 1$$
$$x^6 = x(x^2 + x + 1) = \ldots = x^2 + 1$$
$$x^7 = x(x^2 + 1) = x^3 + x = 1$$

With this rule it is clear that any nonzero element of the field can be identified to one of the x^i with $i \in \{1,\ldots,7\}$. (Note that $x^3 + x + 1$ is an irreducible polynomial over Z_2: this is the essential ingredient to get a field.)

Principle of the coding with a field K having elements:

We code words of m letters, the letters being elements $k_1,\ldots,k_m$ of K by transforming them in words of 2^n elements. As before the non zero elements of K can be written in the form $\{x,x^2,\ldots,x^{2^n-1}\}$. The first letter is k_1, while the $2^n - 1$ remaining letters are given by

$$k_1 + k_2x^i + \ldots + k_mx^{i(m-1)}, \; i = 1,\ldots,2^n - 1 .$$

This codes corrects:

$$\frac{2^n - m}{2} \text{ errors if } m \text{ even}$$

$$\frac{2^n - m - 1}{2} \text{ errors if } m \text{ odd}$$

In particular if $n = 3$ (K has 8 elements) and $m = 4$, a word of 4 letters is encoded in a word of 8 letters and the code corrects 2 errors.

Applications:

This code is usually applied with a field of 256 elements (polynomials are multiplied modulo an irreducible polynomial of degree 8 ever z_2). Important applications are, for instance, the communication with satellites. Also Reed-Solomon codes are used when recording music on compact disks.

Image compression

The simplest way to keep an image in memory is to give the color of each pixel. *An enormous memory is needed as soon as we deal with many images!*

How to do better?

Suppose we have drawn a city. We keep in memory ...

Line segments;
Circles arcs;
etc.

... which approximate our image.

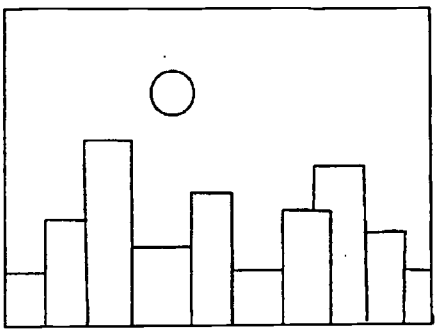

FIGURE 3:
A city

We have approximated our image with known geometric objects.

To keep a line segment in memory it is more economical to keep in memory

- the two ends of the segments;
- a program which tells the computer how to draw the line segment joining two points.

The geometric objects are our *alphabet*.

How can we keep in memory a complex landscape?

We use the same principle with a larger alphabet, i.e.,

- we approximate our landscape with fractals, for instance the fern;
- we keep in memory the program for drawing the fractals, for instance the fern. Because the fern is auto similar the program is less than 15 lines long.

Principle to draw the fern:

The fern is a union:

- of a tail,
- of 3 smaller ferns.

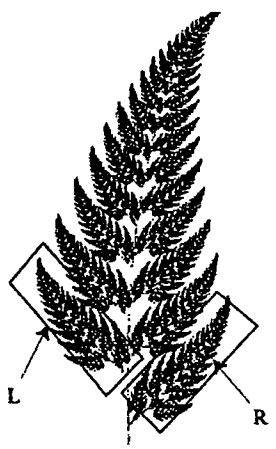

FIGURE 4:
The fern

We can reconstruct the fern from 4 affine transformations:

- the transformation T_1 which sends the large fern to the fern without the two smaller branches;
- the transformation T_2 which sends the large fern to the small left fern;
- the transformation T_3 which sends the large fern to the small right fern;
- the transformation T_4 which sends the large fern to the tail.

It suffices to keep this information in memory to reconstruct the fern. The method is called "Iterated functions systems" [B].

Algorithm:

- we start with P on the fern;
- we choose at random $i_1 \in \{1,2,3,4\}$; we draw $P_1 = T_{i_1}(P)$;
- we choose at random $i_2 \in \{1,2,3,4\}$; we draw $P_2 = T_{i_2}(P_1)$;
- etc. ...

Vision of computers

We treat here just one small aspect which consists in understanding 3D-space from 2D-images.

We have two pictures taken by two different observers located at O_1 and O_2. In our model the images of P are respectively P_1 and P_2. These points are located at the intersection of the lines D_1 and D_2 joining respectively P to O_1 and O_2 with the projection planes (in our figure we took the same projection plane for the two pictures).

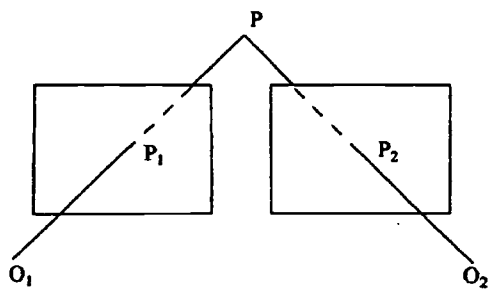

FIGURE 5:
The two pictures

- From the knowledge of P_1 we know that the observed point is on D_1.
- From the knowledge of P_2 we know that the observed point is on D_2.
- The lines D_1 and D_2 have only one intersection point. Hence we know the position of P.

This is what we do all the time: we need two eyes to evaluate deepness: our brain makes the calculation from two images. We need to understand the mechanism to teach computers to do the same.

Exercises:

The exercises done in the course had to do with the images of straight lines and circles in the picture and with perspective.

The movements of a robot

A 3-dimensional robot: *six degrees of freedom are necessary to bring the grip to its position.*

Reflection on the number of degrees of freedom:

- movements 1, 2, and 3 bring P to its position;
- movements 4 and 5 bring the axis of the grip to its position;
- movement 6 brings the grip to its final position by a rotation around its axis.

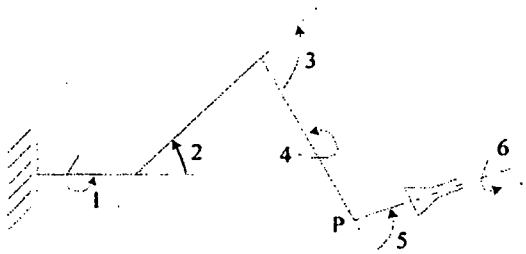

FIGURE 6: Example of a robot with 6 degrees of freedom

Exercises: reflection!

- The construction of the robot is not unique but 6 degrees of freedom (so at least 6 independent movements) are necessary to reach any point in a given region of the space with the grip properly oriented. So 6 degrees of freedom are also necessary for the handles with which one controls the robot.
- Try to imagine other models of robots with 6 degrees of freedom.
- How many degrees of freedom are necessary for a robot moving only in the plane (the answer depends on the problem, namely the different positions of the grip which are necessary to achieve the job)?
- Depending on the length of the different parts of the robot, what points of the plane (space) can be reached by the grip?

The underlying mathematics:

- Each movement is a rotation $R_i(\theta_i)$ in coordinates (x_i,y_i,z_i) centered in P_i.
- It is represented by a matrix $M_i(\theta_i)$.
- We change from one coordinate system to another by a translation followed by a rotation.
- This allows us to know the coordinates of a given point Q in each coordinate system.
- In particular we can calculate the position of Q in the original system after rotations $R_i(\theta_i)$, $i \in \{1,2,3,4,5,6\}$. This involves matrix multiplications.
- Hence we know the effect of a composition of movements on any point. All operations can be inverted.

Exercises:

Imagine problems for an engineer. For instance:

- There exists several sequences of movements bringing the robot to the same final position. Which is best? Some "small" movements lead to "large" displacements of the grip, while some "large" movements lead to "small" displacements of the grip. The latter are better when doing precision work.
- We may add extra pieces and movements in order to allow the robot to go around obstacles. What is the effect of adding pieces and increasing the number of possible movements?
- What is the effect of changing the length of some of the pieces?
- Inverse problem (difficult!): Given a final position of the grip give a sequence of movements to bring the grip to this position. This yields to solving a system of nonlinear equations.

Application:

The Canadian arm for the international spacel station.

References

[B] M. Barnsley. (1988). *Fractals everywhere.* New York: Academic Press.

[C] J. Cox. (1992). The shape of the ideal column. *Mathematical Intelligencer,* 14, 16–24.

[GPS] http://www.trimble.com/gps/fsections/aa.f1.htm
http://www.mercat.com/QUEST/gpstutor.htm

http://www.colorado.edu/geography/gcraft/notes/gps/gps.f.html

[RS] I.S. Reed & G. Solomon. (1960). Polynomial codes over certain fields. *Journal of the Society for Industrial and Applied Mathematics*, , 300–304.

[RSA] R.L. Rivest, A. Shamir, & L. Adleman. (1978). A method for obtaining digital signatures and public key cryptosystems. *Communications of the ACM*, 21(2), 120–126.

[R] C. Rousseau. (2000). Théorie des nœuds et chaînes d'ADN. Collectif « *Mathématiques d'hier et d'aujourd'hui* », Modulo Éditeur.

SE066374

U.S. Department of Education
Office of Educational Research and Improvement (OERI)
National Library of Education (NLE)
Educational Resources Information Center (ERIC)

REPRODUCTION RELEASE
(Specific Document)

I. DOCUMENT IDENTIFICATION:

Title: CANADIAN MATHEMATICS EDUCATION STUDY GROUP PROCEEDINGS 2001 ANNUAL MEETING	
Author(s): ELAINE SIMMT, BRENT DAVIS, JOHN GRANT MCLOUGHLIN (Eds)	
Corporate Source: Canadian Mathematics Education Study Group	Publication Date: 2002

II. REPRODUCTION RELEASE:

In order to disseminate as widely as possible timely and significant materials of interest to the educational community, documents announced in the monthly abstract journal of the ERIC system, *Resources in Education* (RIE), are usually made available to users in microfiche, reproduced paper copy, and electronic media, and sold through the ERIC Document Reproduction Service (EDRS). Credit is given to the source of each document, and, if reproduction release is granted, one of the following notices is affixed to the document.

If permission is granted to reproduce and disseminate the identified document, please CHECK ONE of the following three options and sign at the bottom of the page.

The sample sticker shown below will be affixed to all Level 1 documents	The sample sticker shown below will be affixed to all Level 2A documents	The sample sticker shown below will be affixed to all Level 2B documents
PERMISSION TO REPRODUCE AND DISSEMINATE THIS MATERIAL HAS BEEN GRANTED BY Sample TO THE EDUCATIONAL RESOURCES INFORMATION CENTER (ERIC) 1	PERMISSION TO REPRODUCE AND DISSEMINATE THIS MATERIAL IN MICROFICHE, AND IN ELECTRONIC MEDIA FOR ERIC COLLECTION SUBSCRIBERS ONLY, HAS BEEN GRANTED BY Sample TO THE EDUCATIONAL RESOURCES INFORMATION CENTER (ERIC) 2A	PERMISSION TO REPRODUCE AND DISSEMINATE THIS MATERIAL IN MICROFICHE ONLY HAS BEEN GRANTED BY Sample TO THE EDUCATIONAL RESOURCES INFORMATION CENTER (ERIC) 2B
Level 1	**Level 2A**	**Level 2B**
Check here for Level 1 release, permitting reproduction and dissemination in microfiche or other ERIC archival media (e.g., electronic) *and* paper copy.	Check here for Level 2A release, permitting reproduction and dissemination in microfiche and in electronic media for ERIC archival collection subscribers only	Check here for Level 2B release, permitting reproduction and dissemination in microfiche only

Documents will be processed as indicated provided reproduction quality permits.
If permission to reproduce is granted, but no box is checked, documents will be processed at Level 1.

I hereby grant to the Educational Resources Information Center (ERIC) nonexclusive permission to reproduce and disseminate this document as indicated above. Reproduction from the ERIC microfiche or electronic media by persons other than ERIC employees and its system contractors requires permission from the copyright holder. Exception is made for non-profit reproduction by libraries and other service agencies to satisfy information needs of educators in response to discrete inquiries.

Signature: c/c E. SIMMT	Printed Name/Position/Title: Proceedings Editor
Organization/Address: 341 Education South University of Alberta Edmonton, Alberta CANADA T6G 2G5	Telephone: 780.492.0858 FAX: 780.492.9402
	E-Mail Address: elaine.simmt@ualberta.ca Date: Dec 12/02

III. DOCUMENT AVAILABILITY INFORMATION (FROM NON-ERIC SOURCE):

If permission to reproduce is not granted to ERIC, or, if you wish ERIC to cite the availability of the document from another source, please provide the following information regarding the availability of the document. (ERIC will not announce a document unless it is publicly available, and a dependable source can be specified. Contributors should also be aware that ERIC selection criteria are significantly more stringent for documents that cannot be made available through EDRS.)

Publisher/Distributor:
Address: na
Price:

IV. REFERRAL OF ERIC TO COPYRIGHT/REPRODUCTION RIGHTS HOLDER:

If the right to grant this reproduction release is held by someone other than the addressee, please provide the appropriate name and address:

Name: na
Address:

V. WHERE TO SEND THIS FORM:

Send this form to the following ERIC Clearinghouse:

However, if solicited by the ERIC Facility, or if making an unsolicited contribution to ERIC, return this form (and the document being contributed) to:

ERIC Processing and Reference Facility
4483-A Forbes Boulevard
Lanham, Maryland 20706

Telephone: 301-552-4200
Toll Free: 800-799-3742
FAX: 301-552-4700
e-mail: ericfac@inet.ed.gov
WWW: http://ericfacility.org